



Programación Python para BigData

Lección 9: Quantum Computing

Índice

Primera parte de la Actividad.....	3
Historia de la Computación Cuántica.....	3
Siglo XX.....	3
Siglo XXI.....	3
El Computador cuántico.....	4
El cúbit.....	4
La superposición cuántica.....	4
Entrelazamiento cuántico.....	5
Decoherencia.....	5
Segunda parte de la actividad.....	6
Tercera parte de la actividad.....	7
IF o buffer.....	7
AND.....	8
OR.....	8
XOR.....	8
Cuarta parte de la actividad.....	9
Quinta parte de la actividad.....	10
Sexta parte de la actividad.....	11
Séptima parte de la actividad.....	11

Primera parte de la Actividad

Historia de la Computación Cuántica

Siglo XX

Las primeras ideas de la computación cuántica nacen en los años 80, década en la que, durante la primera convención de física cuántica, el físico Richard Feynman propone, por primera vez, el uso de fenómenos cuánticos para realizar cálculos de alta complejidad de forma más eficiente. Poco después el físico israelí David Deutsch describe el primer computador cuántico capaz de ejecutar diferentes algoritmos cuánticos, los computadores descritos hasta el momento únicamente podían ejecutar un algoritmo. Sin embargo, no sería hasta la década de los noventa que empezarían a aparecer las primeras aplicaciones de esta tecnología, sería entonces cuando el físico Peter Shor definiría el algoritmo que lleva su nombre y mediante el cual demostró que el campo de la computación cuántica poseía un gran potencial. Poco después, comenzarían los experimentos con los que se darían los primeros pasos hacia la computación cuántica al conseguir realizar una comunicación de criptografía cuántica a una distancia de 23 Km. Poco después se lograría propagar el primer cúbit a través de un medio de aminoácidos dando lugar a la posibilidad de analizar la información transmitida por éste y a las primeras máquinas de computación cuántica. La primera se crearía en la Universidad de Berkeley dotada de dos cúbits, el siguiente año, IBM crearía una máquina de tres cúbits capaz de ejecutar por primera vez el algoritmo de Grover.

Siglo XXI

Ya en el nuevo siglo continuarían los progresos, en el año 2000 se ejecutaría con éxito y en un solo paso un algoritmo de búsqueda de orden (parte del algoritmo de Shor) empleando una máquina dotada de 5 cúbits creada una vez más, por IBM. En ese mismo año, Los Álamos National University crearía la primera máquina de 7 cúbits y se conseguiría emular la codificación en bits empleando un resonador magnético nuclear. Un año más tarde IBM junto a Los Álamos conseguirían ejecutar con éxito el algoritmo de Shor para los factores primos de 15. En 2005, los científicos de la universidad de Innsbruck, en Austria, crearían el primer cúbyte que consistía en una agrupación de 8 cúbits enlazados mediante una trampa de iones. Dos años después, se crearía el primer bus cuántico que no solo se emplearía para unir diferentes componentes cuánticos si no también haría las veces de memoria cuántica a corto plazo y un año más tarde, en Estados Unidos se conseguiría por primera vez almacenar la información de un cúbit en el interior del núcleo de un átomo de fósforo durante un periodo de 1,75s. En 2009 un equipo de la universidad de Yale crearía el primer procesador cuántico de estado sólido. Siete años más tarde IBM crearía el primer procesador cuántico comercial, con un poder de procesamiento de 17 cúbits y tres años más tarde, esta misma empresa presentaría el IBM Q System One, el primer computador cuántico de uso comercial.

El Computador cuántico

Una vez hemos analizado la breve historia de la computación cuántica, analicemos que es un computador cuántico y como funciona.

La definición generalizada y mas sencilla que podemos encontrar en las redes es la siguiente:

Un ordenador cuántico es aquel que emplea como unidad básica de información el cúbit en lugar del bit clásico, ofreciendo así un gran aumento en capacidad y potencia de procesamiento.

Pero, ¿a que se debe este “gran aumento en capacidad y potencia de procesamiento”? Para dar respuesta a esta pregunta, primero hay que entender que es un cúbit.

El cúbit

A diferencia de un bit tradicional que únicamente puede representar dos estados, ya que se genera mediante pulsos de distinta índole, un bit cuántico o cúbit, es capaz de presentar una infinidad de estados ya que un cúbit en realidad es partícula elemental, es decir, son partículas que conforman el nivel mas pequeño de la materia, estas partículas se clasifican en tres familias: cuarks, leptones y bosones. Entre todas las partículas elementales, dieciséis en total, para crear un cúbit se emplean fotones o electrones que son, de entre todas, las mas estables y fáciles de obtener. Esto implica que si bien el cúbit posee dos estados fundamentales $|0\rangle$ y $|1\rangle$, cuando se le aplican ciertos algoritmos, cuánticos naturalmente, lo que obtenemos es un valor cuántico que establece que posibilidades tenemos de obtener un $|0\rangle$ ó un $|1\rangle$. Posibilidades, si, el estado de un cúbit no se define hasta que no se mide, al igual que sucede con la paradoja del gato de Schrödinger, el bit cuántico permanece en superposición hasta que se realiza una medida, esta es otra de las cualidades que hacen muy útiles a los cúbits.

La superposición cuántica

Entender este concepto es relativamente sencillo si conocemos la paradoja del gato de Schrödinger, la paradoja dice lo siguiente:

Imaginemos que tenemos un gato en una caja en la que metemos un vial de gas venenoso y un martillo justo encima del vial, el martillo esta sujeto por un mecanismo que lo dejara caer si detecta alguna partícula radiactiva. Además, en la caja incluimos otra caja sellada más pequeña en la que se ha introducido un elemento radiactivo. Pasado cierto tiempo dado que no es seguro que el detector haya detectado radiación, no sabremos si el gato esta vivo o muerto hasta no abrir la caja, sin embargo podremos saber que probabilidades tiene el gato de estar vivo en función de la precisión del sensor.

Con los cúbits pasa lo mismo, una vez empezamos a aplicar algoritmos, se puede interpretar que lo introducimos en una caja que nos irá mostrando que posibilidades tiene el cúbit de mostrar cualquiera de los dos estados y esto claro está, varia a medida que se aplican algoritmos. ¿Entonces,

eso significa que no se puede nada de un cúbit hasta medirlo? Respuesta corta, no, respuesta larga, no se puede establecer cierta relación entre los cúbits.

Entrelazamiento cuántico


¿Entonces, es posible conocer el estado de un cúbit sin medirlo? Realmente no, pero si se puede establecer una relación entre un par de cúbits de forma que lo que le afecte a uno le afecte al otro y se pueda obtener, hasta cierto punto, un resultado predecible, a este fenómeno se le denomina Entrelazamiento Cuántico. Mediante este fenómeno se puede establecer por ejemplo que el cúbit “A” se al opuesto al cúbit “B” de forma que si el cúbit “A” finalmente devuelve un estado $|0\rangle$, el cúbit “B” devolverá un estado $|1\rangle$, de esta forma es posible “predecir” hasta cierto punto el resultado de una medición dando igual la distancia ya que no afecta en absoluto la distancia a la que se encuentren ambos cúbits.

Decoherencia

Hasta ahora hemos visto que los cúbits tienen propiedades bastante interesantes sin embargo, todo esto tiene un “pero” muy a tener en cuenta y es que es estado de un cúbit, por ser cuántico, es altamente inestable es por ello que los ordenadores cuánticos necesitan estar en entornos muy controlados en los que cada parámetro del mismo esté controlado, ya que la temperatura ha de ser cercana al Cero Absoluto y no puede filtrarse ningún tipo de onda ni señal de tipo alguno ya que podrían desde cambiar el estado del cúbit hasta hacerlo desaparecer.


Segunda parte de la actividad

Welcome, [REDACTED]



Graphically build circuits with
IBM Quantum Composer



Launch Composer




Develop quantum experiments in
IBM Quantum Lab

Launch Lab

Get started locally ⓘ
Your API token


*****  

[View account details](#)




Run on circuits & algorithms via
IBM Quantum services [View all](#)

6	7	5	34
Your programs	Your systems	Your simulators	Total quantum services

 **Reservations**

0

Your reservations

 **Recent jobs** [View all](#)

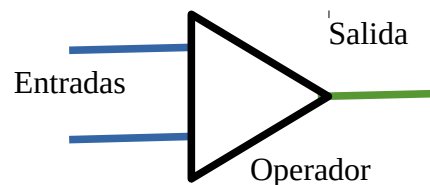
You have no recent jobs.

Create one by running a circuit or notebook on one of your IBM Quantum Systems.

Tercera parte de la actividad

Antes de existir la programación a base de código, existía una forma más simple de programar autómatas, emplear la puertas lógicas. Estas puertas consisten con conjuntos de contactos que según estén abiertos o cerrados dan señal o no a la salida.

Las puertas lógicas constan de tres zonas, las entradas, el operador y la salida, en un diagrama sería del siguiente modo:



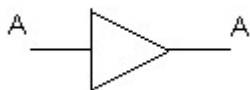
Se clasifican en cuatro tipos, AND, OR, IF y XOR, además de ello cada una tiene su versión negada que consiste en la “apagar” la salida que de no estar negada estaría “encendida”, las analizaremos una por una pero antes es necesario introducir otro concepto, la tabla de verdad.

La tabla de verdad es una tabla que muestra el comportamiento de las puertas lógicas en función de que entrada tienen activa, de modo que con un simple vistazo es posible analizar el comportamiento de estas ante una situación dada.

Ahora si, analicemos las puertas y sus tipos:

IF o buffer

Es la única puerta con una única entrada y devuelve señal si su entrada está activa:



SI

Entrada A	Salida A
0	0
1	1

AND

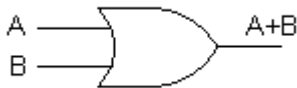
Activa la salida únicamente si ambas entradas están activas, es la representación física de una multiplicación binaria:



Entrada A	Entrada B	Salida $A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

OR

Activa la salida si, cualquiera de ambas entradas está activa o si ambas lo están activas, también es la representación de la suma binaria.



Entrada A	Entrada B	Salida $A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

XOR

Puerta or exclusiva, activa la salida únicamente si una única de las entradas está activa, es la representación de la resta binaria.



Entrada A	Entrada B	Salida $A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Las puertas negadas no las explicaremos ya que su funcionamiento es el mismo salvo que invierten la señal de la salida, en las tablas de verdad donde aparece un uno, se pone un 0 y viceversa.

Cuarta parte de la actividad

Las puertas lógicas cuánticas son a los computadores cuánticos lo que las puertas lógicas a los ordenadores clásicos es decir, las puertas lógicas cuánticas son pequeños operadores que actúan sobre un pequeño grupo de cúbits. Presentan ciertas diferencias respecto a las puertas clásicas de entrada, las puertas cuánticas son reversibles y a diferencia de las clásicas, no pueden ser representadas por operadores simples, han de ser representadas por matrices. Estas matrices son matrices 2×2 ó 4×4 unitarias y ortonormales, el hecho de que sean unitarias es precisamente lo que le da a las puertas cuánticas su propiedad de reversibles y el hecho de que sean ortonormales implica que los vectores que conforman la matriz son linealmente independientes y que cada uno de sus valores es 1. Dada la complejidad de las matemáticas subyacentes en este tema no analizaremos el funcionamiento de las puertas y mencionaremos las puertas más comunes y en algún caso su funcionamiento.

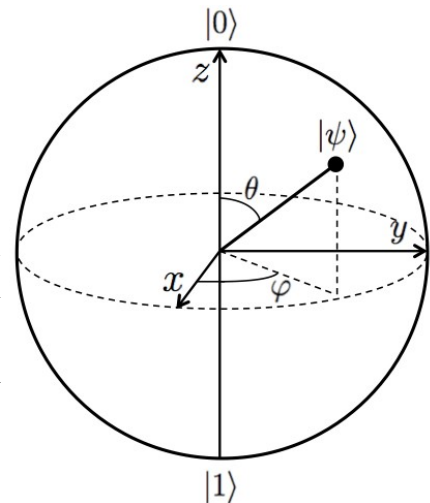
Entre las mas comunes se hallan, la **Hadamard** que realiza un cambio de estado, la **puerta de desplazamiento de fase**, que realiza una rotación sin alterar el estado del cúbit y la **puerta swap** intercambia dos cúbits, las **puertas controladas** controlan el estado de un grupo de cúbits en función de un único cúbit.

Quinta parte de la actividad

Antes de definir lo que es una esfera de Bloch definamos ciertos conceptos necesarios. Un **estado físico** o **estado puro** se define como aquel estado o situación de un sistema físicamente distinguible del resto de estados del mismo sistema.

Teniendo esto en cuenta pasemos a la esfera de Bloch: Una esfera de Bloch es un espacio de \mathbf{R}^3 o espacio tridimensional de estados puros que un cúbit puede adoptar, se emplea una esfera para representar los estado de un cúbit ya que tiene tres ejes y gracias a ello presenta ciertas características muy interesantes como son las rotaciones sobre un eje sin alterar el estado, la posibilidad del cambio de coordenadas y la facilidad para la medición de ángulos. Las esferas de Bloch se representan mediante la siguiente ecuación:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$



Esta ecuación es una representación en forma angular de un número complejo, que son los números empleados para representar los estados de una esfera de Bloch.

Sexta parte de la actividad

Los números complejos son un conjunto de números que alberga todas y cada una de los números reales y que además contiene al conjunto completo de los números reales, matemáticamente $\mathbf{R} \subset \mathbf{C}$, siendo \mathbf{R} el conjunto de los reales y \mathbf{C} el conjunto de los complejos además, todo numero complejo esta formado por un par tal que $z = a + bi$, siendo \mathbf{a} la parte real de \mathbf{z} y \mathbf{b} la parte imaginaria. Se deduce de esta ultima definición que los números complejos, se representan en planos de \mathbf{R}^2 ya que su dimensión mina es 2 y por lo tanto son vectores, llegando así a la conclusión de que para operar con ellos es necesario emplear matemática vectorial.

Séptima parte de la actividad

Al igual que un Algoritmo clásico se encarga de operar sobre una serie de números para otorgar un resultado, los algoritmos cuánticos realizan las mismas operaciones pero tomando como “entrada” elementos como un cúbit. A diferencia de los algoritmos clásicos que entregan un resultado concreto, los algoritmos cuánticos al aplicarlos sobre un cúbit devuelven un valor que nos da una probabilidad de obtener un estado u otro a la salida. Existen algoritmos cuya labor esta predefinida y que se emplean para labores muy concretas, entre los mas famosos están el algoritmo de Shor o el algoritmo de Grover.